## REMARKS

Initially, in the Office Action dated March 11, 2004, the Examiner rejects claims 1-3, 5-8, 10, 11, 27-29, 32, 35-38, 40, 41 and 44 under 35 U.S.C. §102(b) as being anticipated by EP 0673178 A2 (Ohashi). Claims 4, 34 and 42 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ohashi in view of Applied Cryptography (Schneier). Claims 12-16, 30 and 31 have been rejected under 35 U.S.C. §103(a) over Ohashi in view of U.S. Patent No. 6,522,880 (Verma et al.) Claims 17 and 33 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ohashi in view of U.S. Patent No. 5,668,875 (Brown et al.). Claims 9 and 39 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ohashi in view of U.S. Patent No. 5,091,942 (Dent). Claims 18-26 and 43 are objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form to include all of the limitations of the base claim and any intervening claims.

Allowable subject matter

Applicants thank the Examiner for indicating that claims 18-26 and 43 would be allowable if rewritten in independent form to include all of the limitations of the base claim and any intervening claims.

35 U.S.C. §102 Rejections

Claims 1-3, 5-8, 10, 11, 27-29, 32, 35-38, 40, 41 and 44 have been rejected under 35 U.S.C. §102(b) as being anticipated by Ohashi. Applicants respectfully traverse these rejections.

Ohashi discloses a mobile communication authentication method for authenticating a mobile station which accesses for roaming a network different from a home network of the mobile station. The mobile station and the home network have the same secret key and use the same cipher function. The mobile station is preliminarily authenticated by sending from the home network to the roamed network, a plurality of pairs of first random numbers and calculation results of the cipher function. The calculation is performed at the home network using the secret key and the first random numbers. The roamed network sends to the mobile station third random numbers formed by coupling second random numbers produced at the roamed network with the first random numbers. The mobile station sends to the roamed network calculation results of the cipher function. The calculation is performed at the mobile station using the secret key and the third random numbers. The roamed network confirms coincidence of the calculation results sent from the mobile station with the calculation results sent from the home network and authenticates the mobile station by using a pair of the second random number and of the calculation result with respect to the second random number sent from the mobile station.

Regarding claims 1, 27, 29 and 40, Applicants submit that Ohashi does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, delegation of security procedures to a second domain that includes generating a second key at a home domain using the first key and a random number and sending the random number and the second key to the second domain, sending the random

number to the mobile node by the second domain, generating the second key by the mobile node using the random number and the first key, or using the second key for at least one authentication procedure between the mobile node and the second domain. Ohashi discloses sending a plurality of pairs of first random numbers from a home network to a roamed network, the roamed network generating a second set of random numbers and sending the second set of random numbers and the first set of random numbers to the mobile device in a random arrangement where the mobile station performs a calculation on the second and third sets of random numbers using a secret key and cipher function and forwards the result of this calculation to the roamed network, the roamed network authenticating the mobile station using the pair of second random numbers and the calculation result with respect to the second random numbers sent from the mobile station. This is not sending a single random number to the mobile node by the second domain, the mobile node generating a second key using the random number and the second domain using the second key for authentication between the mobile node and the second domain, as recited in the claims of the present application. According to the present invention, a second key and a random number used to generate the second key are sent to a second domain where the second domain forwards the same random number to the mobile node that generates the same second key and returns it to the second domain for authentication. In contrast, Ohashi discloses the roamed network generating a second set of random number pairs and sending this second set along with a first set of random number pairs to the mobile terminal. Thus, the information sent from the

roamed network is different than the information received from the home network. Moreover, the present invention discloses sending a single random number to the mobile node by the second domain. In contrast, Ohashi discloses sending a plurality of pairs of third random numbers formed by coupling second random numbers produced at the roamed network with first random numbers. According to the limitations in the claims of the present application, the random number sent to the mobile node is not modified or coupled to anything in the second domain, in contrast with that disclosed in Ohashi. Ohashi does not disclose or suggest sending the same random number from the home network via the roaming network to the mobile node, as recited in the claims of the present application.

Regarding claims 2, 3, 5-8, 10, 11, 28, 32, 35-38, 41 and 44, Applicants submit that these claims are dependent on one of independent claims 1, 27, 29 and 40 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Applicants submit that Ohashi does not disclose or suggest the authentication procedures comprising authentication of the second domain by the mobile node, or sending the random number and the second key to the second domain across a secure channel.

Accordingly, Applicants submit that Ohashi does not disclose or suggest the limitations in the combination of each of claims 1-3, 5-8, 10, 11, 27-29, 32, 35-38, 40, 41 and 44 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claims 4, 34 and 42 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ohashi in view of Schneier. Applicants respectfully traverse these rejections.

Schneier discloses communications using public key cryptography and specifically, implementations used to secure and distribute session keys that are used with symmetric algorithms to secure message traffic.

Applicants submit that claims 4, 34 and 42 are dependent on one of independent claims 1, 29 and 40 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Schneier does not overcome the substantial defects noted previously regarding Ohashi. For example, none of the cited references disclose or suggest a key derivation procedure as recited in the claims of the present application that generates at least one session key using a second key.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 4, 34 and 42 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 12-16, 30 and 31 have been rejected under 35 U.S.C. §35 U.S.C. §103(a) as being unpatentable over Ohashi in view of Verma et al. Applicants respectfully traverse these rejections.

Verma et al. discloses method and apparatus for handoff of a connection between network devices that includes handing off a communications stream between a mobile node and a communication endpoint from a first connection initiator to a second connection initiator while maintaining call state for the communication stream.

Applicants submit that claims 12-16, 30 and 31 are dependent on one of independent claims 1 and 29 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Verma et al. does not overcome the substantial defects noted previously regarding Ohashi. For example, Applicants submit that none of the cited references disclose or suggest communicating with the mobile node by the AAA server through an AAA client.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 12-16, 30 and 31 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 17 and 33 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ohashi in view of Brown et al. Applicants respectfully traverse these rejections.

Brown et al. discloses method and apparatus for authenticating a roaming subscriber where a subscriber receives a challenge that is in a format of a local

authentication protocol, and determines whether the local authentication protocol is the subscriber's home system authentication protocol. If it is not, the subscriber converts the challenge into a format e.g., bit length, compatible with its home system authentication protocol, and processes the converted challenge with the subscriber's secret key and authentication algorithm into an authentication response.

Applicants submit that claims 17 and 33 are dependent on one of independent claims 1 and 29 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Brown et al. does not overcome the substantial defects noted previously regarding Ohashi. For example, Applicants submit that none of the cited references disclose or suggest the second key being a temporary shared key.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 17 and 33 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 9 and 39 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ohashi in view of Dent. Applicants respectfully traverse these rejections.

Dent discloses a system for the authentication of mobile stations and base stations in a cellular communication network. The system includes an algorithm which generates not only a key dependent response to a random challenge, but also

a temporary conversation key or call variable which may be used to encipher traffic in the network. To protect against clones in the network, the algorithm uses a rolling key which contains historical information.

Applicants submit that claims 9 and 39 are dependent on one of independent claims 1 and 29 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Dent does not overcome the substantial defects noted previously regarding Ohashi. For example, Applicants submit that none of the cited references disclose or suggest the authentication procedures comprising distribution of dynamic keys between the mobile node and entities in the second domain based on a local security association.

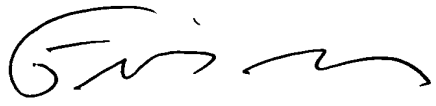
Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 9 and 39 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing remarks, Applicants submit that claims 1-44 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 0172.39681X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600